U.S. Department of Energy
Office of Electricity Delivery and Energy Reliability

Automated Vulnerability Detection for Compiled Smart Grid Software

Improving cybersecurity vulnerability detection for smart grid components and systems

Background

Exploitation of software vulnerabilities in smart grid systems can lead to inaccurate electricity usage reports, privacy issues, power supply problems or opportunities for attacks on other infrastructure components. Vulnerability testing is often used in IT systems to validate proper system configuration and to identify any vulnerabilities that may be present. However, conventional IT vulnerability testing can disable or shut down energy delivery systems and testing does not always detect vulnerabilities hidden deep within a device's control software.

Barriers

- Conducting performance and acceptance testing of energy delivery system components without disrupting real-time operations is difficult
- Current software testing can only provide information about the specific scenarios actually observed

Project Description

This project will develop and demonstrate a system for conducting cybersecurity vulnerability detection of smart grid components and systems by performing static analysis of compiled software and device firmware.

This system will be implemented as part of Oak Ridge National Laboratory's (ORNL's) existing test bed for smart meters, the Sustainable Campus Initiative.

The project is divided into two phases. The first phase will implement the necessary software and computational models to perform the analysis. The second phase will demonstrate the system on firmware and deploy it as part of the test bed. By directly analyzing the compiled software, the system will be able to detect both unintended and maliciously inserted vulnerabilities in smart grid components. Based on this information, mitigations for these vulnerabilities can be recommended.

The initial target for this effort will be the software present in smart meters. While testing can only provide information about the specific scenarios actually observed, static analysis can provide information about the system behavior under any use, and offers a significantly more robust means of vulnerability detection than is available today.

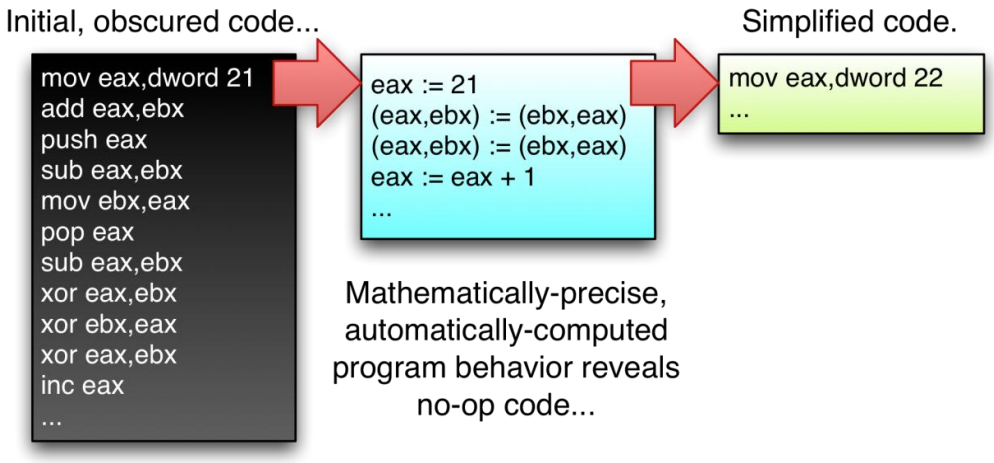
Benefits

- Detects unintended and maliciously inserted vulnerabilities in compiled smart grid software
- Provides information about system behavior under any use
- Detects vulnerabilities that traditional testing may miss
- Enables mitigation recommendations

Partners

- Oak Ridge National Laboratory
- EnerNex Corporation
- Sensus

Exploiting computed behavior for code simplification



Technical Objectives

The core objective of this project is to research, develop and demonstrate a system for conducting cybersecurity vulnerability detection of smart grid components and systems by performing static analysis of compiled software and device firmware. The project is divided into two phases:

Phase One

- Implement software and computational models
- Develop vulnerability model using core algorithms deployed on high-performance hardware

Phase Two

- Create test suite of vulnerability firmware
- Demonstrate system's ability to detect seeded vulnerabilities
- Implement into ORNL test bed

August 2012

End Results

Project results will include:

- More robust vulnerability detection through static analysis of compiled software and device firmware
- Mitigation recommendations due to the vulnerability detection efforts
- An automated system for conducting vulnerability detection of smart grid components and systems

Cybersecurity for Energy Delivery Systems (CEDS)

CEDS projects are funded through the Department of Energy's (DOE) Office of Electricity Delivery and Energy Reliability (OE) R&D Program, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of energy disruptions due to cyber attacks.

For More Information:

Carol Hawk
Program Manager
DOE OE R&D
202-586-3247
carol.hawk@hq.doe.gov

Stacy Prowell
Chief Cyber Security Scientist
Oak Ridge National Laboratory
865-241-8874
prowellsj@ornl.gov

Visit Our Website:

http://energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity